



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11086435 A**(43) Date of publication of application: **30 . 03 . 99**

(51) Int. Cl.

G11B 20/10**G09C 1/00****G09C 1/00****G09C 5/00****H04L 9/32****H04N 1/387****H04N 5/91****H04N 7/08****H04N 7/081**(21) Application number: **10190825**(22) Date of filing: **06 . 07 . 98**(30) Priority: **07 . 07 . 97 JP 09181459**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**(72) Inventor: **IBARAKI SUSUMU
KATSUTA NOBORU**

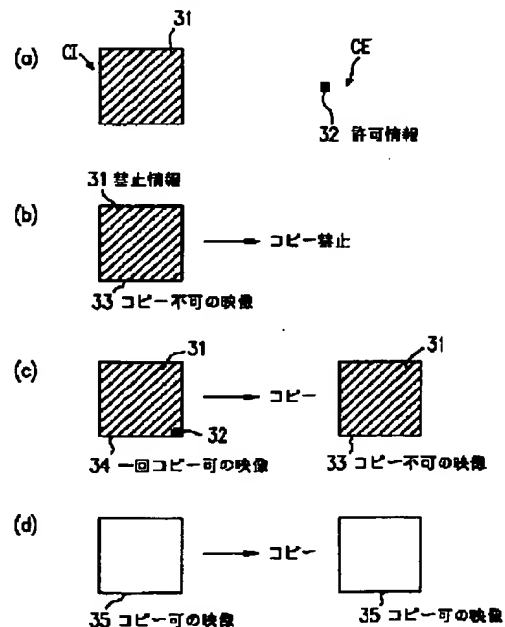
(54) **DATA CONTROL METHOD, DATA CONTROL INFORMATION EMBEDDING METHOD, DATA CONTROL INFORMATION DETECTION, DATA CONTROL INFORMATION EMBEDDING DEVICE, DATA CONTROL INFORMATION DETECTOR AND RECORDER**

COPYRIGHT: (C)1999,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To control copying propriety and the number of copying times and to protect a copyright by embedding prohibition information into data, such as videos and voices.

SOLUTION: The prohibition information 31 is embedded into the videos and permission information 32 is embedded therein by using digital signature, etc., if N times of copying is okay. At the time of reproduction of the data, the presence or absence of the permission information 32 is investigated and a permission flag is set at a 1 or 0. If the permission flag is 1, the permission information 32 is deleted and the copying of the data is made possible. If the permission flag is 0, the prohibition information 31 is detected. A prohibition flag is then made 1 or 0. If the prohibition flag is 1, a copying okay or denial flag is set at the 0 and the copying of the data is prohibited.



(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開平11-86435

(43)公開日 平成11年(1999) 3 月30日

(51)Int.Cl.⁹

識別記号

F I

G 1 1 B 20/10

G 1 1 B 20/10

F

G 0 9 C 1/00

6 4 0

G 0 9 C 1/00

6 4 0 B

6 6 0

6 6 0 D

5/00

5/00

H 0 4 L 9/32

H 0 4 N 1/387

審査請求 有 請求項の数18 O L (全 16 頁) 最終頁に続く

(21)出願番号 特願平10-190825

(22)出願日 平成10年(1998) 7 月 6 日

(31)優先権主張番号 特願平9-181459

(32)優先日 平 9 (1997) 7 月 7 日

(33)優先権主張国 日本 (J P)

(71)出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72)発明者 茨木 晋

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 勝田 昇

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

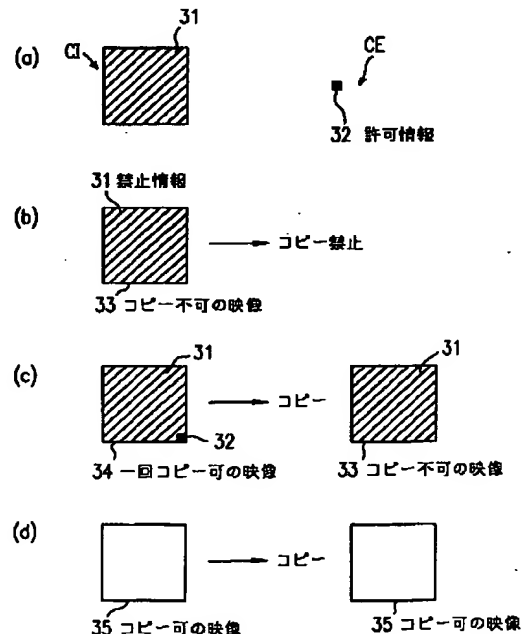
(74)代理人 弁理士 山本 秀策

(54)【発明の名称】 データ制御方法、データ制御情報埋込方法、データ制御情報検出方法、データ制御情報埋込装置、データ制御情報検出装置及び記録装置

(57)【要約】

【課題】映像や音声などのデータにコピー禁止情報を埋め込むことにより、コピー可否やコピー回数の制御を行い、著作権を保護すること。

【解決手段】禁止情報31を映像に埋め込み、N回コピー可ならデジタル署名等を用いて許可情報32を埋め込む。データの再生時には、許可情報32の有無を調べ、許可フラグを1又は0に設定する。許可フラグが1であれば、許可情報32を削除し、データのコピーを可能にする。許可フラグが0であれば、禁止情報31を検出する。そして禁止フラグを1又は0にする。禁止フラグが1であれば、コピー可否フラグを0にし、データのコピーを禁止する。



【特許請求の範囲】

【請求項1】 データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、
前記データのコピーをN（Nは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込み、
前記データのコピーに先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも1つの前記許可情報を無効にして前記データのコピーを許可し、
前記データのコピーに先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データのコピーを禁止することを特徴とするデータ制御方法。

【請求項2】 前記許可情報は、デジタル署名f（M）であって、
前記デジタル署名f（M）は、前記データからデジタルコードMを抽出し、該デジタルコードMに基づいて求められることを特徴とする請求項1記載のデータ制御方法。

【請求項3】 データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、
前記データのコピーをN（Nは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込むことを特徴とするデータ制御情報埋込方法。

【請求項4】 前記許可情報は、
前記データから一意に得られるデジタルコードMに対するデジタル署名f（M）であることを特徴とする請求項3記載のデータ制御情報埋込方法。

【請求項5】 データのコピーに先立ち、前記データから予め定められた許可情報が検出された場合には、前記許可情報を無効にして前記データのコピーを許可し、
前記データのコピーに先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データのコピーを禁止することを特徴とするデータ制御情報検出方法。

【請求項6】 データのコピーに先立ち、前記データ中のデジタル署名f（M）を認証できた場合には、前記データのコピーを許可し、
前記データのコピーに先立ち、前記データ中のデジタル署名f（M）を認証できない場合には、前記データのコピーを禁止し、
前記署名f（M）は、前記データから得られるデジタルコードMに基づいて認証されることを特徴とするデータ制御情報検出方法。

【請求項7】 データの少なくともコピーの禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、
前記データのコピーをN（Nは自然数）回許可したいと

き、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、N個の許可情報を前記データ中に埋め込む許可情報埋込手段と、を具備することを特徴とするデータ制御情報埋込装置。

【請求項8】 前記許可情報埋込手段は、
前記データからデジタルコードMを抽出するコード抽出手段を有することを特徴とする請求項7記載のデータ制御情報埋込装置。

【請求項9】 前記許可情報埋込手段は、前記コード抽出手段で抽出された前記デジタルコードM、及び前記データの作成者が保持する第1の暗号鍵に基づいてデジタル署名f（M）を生成する署名手段と、
前記署名手段で生成されたデジタル署名f（M）を前記許可情報として前記データ中に埋め込む署名埋込手段と、を有することを特徴とする請求項8記載のデータ制御情報埋込装置。

【請求項10】 データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、
前記データから前記許可情報を検出する許可情報検出手段と、
前記データの前記許可情報を無効にする許可情報無効手段と、
前記データから前記禁止情報を検出する禁止情報検出手段と、
前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段と、を具備することを特徴とするデータ制御情報検出装置。

【請求項11】 前記許可情報検出手段は、
前記データからデジタルコードMを抽出するコード抽出手段を有することを特徴とする請求項10記載のデータ制御情報検出装置。

【請求項12】 前記許可情報検出手段は、
前記データに埋め込まれたデジタル署名f（M）を抜き出す署名抜出手段と、
前記コード抽出手段によって抽出された前記デジタルコードMと第2の暗号鍵に基づいてデジタル署名f（M）を生成し、この生成されたデジタル署名f（M）と前記署名抜出手段によって抜き出された前記デジタル署名f（M）を対比し、これによって前記デジタル署名f（M）が認証された場合にコピー許可フラッグを有効にして出力する認証手段と、を具備することを特徴とする請求項11記載のデータ制御情報検出装置。

【請求項13】 データを記録媒体に記録する記録装置であって、
前記データから前記許可情報を検出する許可情報検出手段と、

前記データの前記許可情報を無効にする許可情報無効手段と、
 前記データから前記禁止情報を検出する禁止情報検出手段と、
 前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段と、
 前記判定手段によって前記コピー可否フラッグ許可とされた場合はデータの記録を行い、前記コピー可否フラッグが不可とされた場合は記録を行わないデータ記録手段と、を具備することを特徴とする記録装置。

【請求項14】 データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、
 前記データの処理をN（Nは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込み、
 前記データの処理に先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも1つの前記許可情報を無効にして前記データの処理を許可し、
 前記データの処理に先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データの処理を禁止することを特徴とするデータ制御方法。

【請求項15】 データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、
 前記データの処理をN（Nは自然数）回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込むことを特徴とするデータ制御情報埋込方法。

【請求項16】 データの処理に先立ち、前記データから予め定められた許可情報が検出された場合には、前記許可情報を無効にして前記データの処理を許可し、
 前記データの処理に先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データの処理を禁止することを特徴とするデータ制御情報検出方法。

【請求項17】 データの処理の禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、
 前記データの処理をN（Nは自然数）回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、N個の許可情報を前記データ中に埋め込む許可情報埋込手段と、を具備することを特徴とするデータ制御情報埋込装置。

【請求項18】 データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、
 前記データからN（Nは自然数）個の許可情報が検出さ

れたときには、前記データの少なくとも1つの前記許可情報を無効にし、許可フラッグを有効にして出力する許可情報検出・削除手段と、
 前記データから禁止情報が検出されたときには、禁止フラッグを有効にして出力する禁止情報検出手段と、
 前記許可フラッグが有効か、又は前記禁止フラッグが有効でないときに、可否フラッグを可にして出力し、前記許可フラッグが有効でなく、かつ前記禁止情報が有効であるときに、前記可否フラッグを不可にして出力する判定手段と、
 を具備することを特徴とするデータ制御情報検出装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、音声ソフトや映像ソフトなどに代表される著作権の保護の対象となるデータを、複製（コピー）又はデータ処理（編集）することを防止するため、記録データの複製の許可又は不許可の制御を行うコピー制御情報を付加するデータ制御情報埋め込み方法及びその装置と、その情報を抽出するデータ制御情報検出方法及びその装置と、データ制御情報埋め込み方法及びデータ制御情報検出方法を併せたデータ制御方法とに関するものである。

【0002】

【従来の技術】 映像にコピー制御情報を埋め込む方法として、またコピー制御情報の検出方法として、パッチワークと呼ばれる方法がある。この方法は、日経エレクトロニクスの1997年2月24日号（NO. 683）の149p～162pの「電子透かしを支えるデータハイディング技術（上）」（及びW. Bender, D. Gruhl, N. Morimoto, A. Lu. “Techniques for data hiding”, IBM Systems Journal, Vol 35, NOS 3&4, 1996）に紹介されている。以下、従来技術におけるコピー制御情報埋め込み方法と、その情報を抽出するコピー制御情報検出方法について説明する。

【0003】 従来のコピー制御情報埋込方法として、1枚の映像にコピー可否ビット（1ビット）を埋め込む手順を説明する。コピー可否ビットとして、コピーが可のときは1、コピーが不可のときは0とする。擬似乱数により映像から2点（ A_i 、 B_i ）を選ぶ。次に、埋め込むビットが1のときは、 A_i の輝度レベル Y_{a_i} をdだけ上げ、 B_i の輝度レベル Y_{b_i} をdだけ下げる。逆に、埋め込むビットが0の時は、 A_i の輝度レベルをdだけ下げ、 B_i の輝度レベルをdだけ上げる。このときdの値は1～5の間の整数である。これらの処理をn回（nは通常1万程度）繰り返す。

【0004】 次に従来のコピー制御情報検出方法を説明する。まず、擬似乱数により映像から情報埋込時と同じ位置の2点の輝度レベル（画素情報）、即ち（ $Y_{a_i} + d$ 、 $Y_{b_i} - d$ ）又は（ $Y_{a_i} - d$ 、 $Y_{b_i} + d$ ）を抽出する。そしてこれら2点の差を計算する。これらの処理を夫々の位置についてn回繰り返し、これらの差の平

均を求める。この平均が d 以上であれば、埋め込まれているビットが 1 であるとし、 $-d$ 以下であれば埋め込まれているビットが 0 であるとする。平均が $-d$ 以上、 d 以下のとき、情報が埋め込まれていないとする。

【0005】ここでは、 $Y_{ai} - Y_{bi}$ の期待値を 0 と推定している。また $(Y_{ai} + d) - (Y_{bi} - d)$ の期待値は $2d$ 、 $(Y_{ai} - d) - (Y_{bi} + d)$ の期待値は $-2d$ である。これにより、平均値 0 からのずれの閾値を、 d 及び $-d$ として判定を行っている。更に正確な判定を行うためには、差の統計分布を求め、分散の推定値からのずれによっても、検出可能である。

【0006】以上の様に、従来のコピー制御情報埋込方法及びコピー制御情報検出方法によれば、1 ビットのコピー可否フラグの埋め込みと検出が可能である。更なる方法として、選択した画素に様にレベル d を加算や減算を行うのではなく、映像の特徴に応じて画素ごとに埋め込むレベルを変化させつつ、それらのレベルを各画素の輝度に減算あるいは加算し、これらの平均がレベル d となるようにして情報を埋め込めば、埋め込んだ後の映像の劣化を抑え、不正行為を更に困難にすることができる。

【0007】

【発明が解決しようとする課題】しかるに、コピー制御情報埋込方法および検出方法においては、コピーの許可、禁止を示すだけではなく、コピーを N 回だけ許可するようなコピー回数を制御することが要求されている。コピー回数を制御するには、コピー時にコピー制御情報の書き換えが必要である。例えば、1 回コピー可能なソフトには、1 回コピー可能であることを示すコピー制御情報を埋め込む。そしてコピー時にこれをコピー禁止であることを示すコピー制御情報に書き換えなければならない。

【0008】このようなコピー制御情報の書き換えを、従来のコピー制御情報埋込方法及びコピー制御情報検出方法で実現するためには、コピー制御情報埋込方法とコピー制御情報検出方法の両方をユーザのコピー時に実行しなければならない。従来のコピー制御情報埋込方法は、コピー制御情報検出方法に比べて処理が困難であるので、ユーザが実現するのはコストアップにつながる。また、コピー制御情報埋込方法をユーザに公開することになるので、不正行為が容易に実行される恐れがある。

【0009】本発明は、このような従来の問題点に鑑みてなされたものであって、コピーの許可や禁止だけでなく、コピー回数の制御が可能で、不正処理が困難なデータ制御情報埋め込み方法及びその装置と、データ制御情報検出方法及びその装置を実現することを目的とする。またデータの編集や表示等のデータ処理を制限するデータ制御情報埋め込み方法及びその装置と、データ制御情報検出方法及びその装置を実現することも目的とする。

【0010】

【課題を解決するための手段】このような課題を解決するため、本発明のデータ制御方法は、データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、前記データのコピーを N (N は自然数) 回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、 N 個の許可情報を前記データ中に埋め込み、前記データのコピーに先立ち、前記データから前記許可情報が検出された場合には、前記データの少なくとも 1 つの前記許可情報を無効にして前記データのコピーを許可し、前記データのコピーに先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データのコピーを禁止している。

【0011】1 実施形態では、前記許可情報は、デジタル署名 $f(M)$ であって、前記デジタル署名 $f(M)$ は、前記データからデジタルコード M を抽出し、該デジタルコード M に基づいて求められる。

【0012】本発明のデータ制御情報埋込方法は、データのコピーを禁止する場合は禁止情報を前記データ中に埋め込み、前記データのコピーを N (N は自然数) 回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、 N 個の許可情報を前記データ中に埋め込んでい

る。

【0013】1 実施形態では、前記許可情報は、前記データから一意に得られるデジタルコード M に対するデジタル署名 $f(M)$ である本発明のデータ制御情報検出方法は、データのコピーに先立ち、前記データから予め定められた許可情報が検出された場合には、前記許可情報を無効にして前記データのコピーを許可し、前記データのコピーに先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データのコピーを禁止している。

【0014】1 実施形態では、データのコピーに先立ち、前記データ中のデジタル署名 $f(M)$ を認証できた場合には、前記データのコピーを許可し、前記データのコピーに先立ち、前記データ中のデジタル署名 $f(M)$ を認証できない場合には、前記データのコピーを禁止し、前記署名 $f(M)$ は、前記データから得られるデジタルコード M に基づいて認証される。

【0015】本発明のデータ制御情報埋込装置は、データの少なくとも 1 回のコピーの禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、前記データのコピーを N (N は自然数) 回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、 N 個の許可情報を前記データ中に埋め込む許可情報埋込手段とを具備している。

【0016】1 実施形態では、前記許可情報埋め込み手段は、前記データからデジタルコード M を抽出するコード抽出手段を有する。

【0017】1 実施形態では、前記許可情報埋込手段は、前記コード抽出手段で抽出された前記デジタルコー

ドM、及び前記データの作成者が保持する第1の暗号鍵に基づいてデジタル署名f(M)を生成する署名手段と、前記署名手段で生成されたデジタル署名f(M)を前記許可情報として前記データ中に埋め込む署名埋込手段とを有する。

【0018】本発明のデータ制御情報検出装置は、データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、前記データから前記許可情報を検出する許可情報検出手段と、前記データの前記許可情報を無効にする許可情報無効手段と、前記データから前記禁止情報を検出する禁止情報検出手段と、前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段とを具備している。

【0019】1実施形態では、前記許可情報検出手段は、前記データからデジタルコードMを抽出するコード抽出手段を有する。

【0020】1実施形態では、前記許可情報検出手段は、前記データに埋め込まれたデジタル署名f(M)を抜き出す署名抜出手段と、前記コード抽出手段によって抽出された前記デジタルコードMと第2の暗号鍵に基づいてデジタル署名f(M)を生成し、この生成されたデジタル署名f(M)と前記署名抜出手段によって抜き出された前記デジタル署名f(M)を対比し、これによって前記デジタル署名f(M)が認証された場合にコピー許可フラッグを有効にして出力する認証手段とを具備している。

【0021】本発明の記録装置は、データを記録媒体に記録する記録装置であって、前記データから前記許可情報を検出する許可情報検出手段と、前記データの前記許可情報を無効にする許可情報無効手段と、前記データから前記禁止情報を検出する禁止情報検出手段と、前記許可情報検出手段によって前記許可情報が検出された場合には、コピー可否フラッグを可にして出力し、前記許可情報検出手段によって前記許可情報が検出されずに、前記禁止情報検出手段によって前記禁止情報が検出された場合には、前記コピー可否フラッグを不可にして出力する判定手段と、前記判定手段によって前記コピー可否フラッグ許可とされた場合はデータの記録を行い、前記コピー可否フラッグが不可とされた場合は記録を行わないデータ記録手段とを具備している。

【0022】本発明のデータ制御方法は、データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、前記データの処理をN(Nは自然数)回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込み、前記データの処理に先立ち、前記データから前記許可情報が検出された場

合には、前記データの少なくとも1つの前記許可情報を無効にして前記データの処理を許可し、前記データの処理に先立ち、前記データから前記許可情報が検出されず、前記禁止情報が検出された場合には、前記データの処理を禁止している。

【0023】本発明のデータ制御情報埋込方法は、データの処理を禁止する場合は禁止情報を前記データ中に埋め込み、前記データの処理をN(Nは自然数)回許可する場合は前記禁止情報を前記データ中に埋め込むと共に、N個の許可情報を前記データ中に埋め込んでいる。

【0024】本発明のデータ制御情報検出方法は、データの処理に先立ち、前記データから予め定められた許可情報が検出された場合には、前記許可情報を無効にして前記データの処理を許可し、前記データの処理に先立ち、前記データから前記許可情報が検出されず、予め定められた禁止情報が検出された場合には、前記データの処理を禁止している。

【0025】本発明のデータ制御情報埋込装置は、データの処理の禁止を示す禁止情報を前記データ中に埋め込む禁止情報埋込手段と、前記データの処理をN(Nは自然数)回許可したいとき、前記禁止情報埋込手段による禁止情報の埋め込みに伴い、N個の許可情報を前記データ中に埋め込む許可情報埋込手段とを具備している。

【0026】本発明のデータ制御情報検出装置は、データに埋め込まれた禁止情報及び許可情報を抽出するデータ制御情報検出装置であって、前記データからN(Nは自然数)個の許可情報が検出されたときには、前記データの少なくとも1つの前記許可情報を無効にし、許可フラッグを有効にして出力する許可情報検出・削除手段と、前記データから禁止情報が検出されたときには、禁止フラッグを有効にして出力する禁止情報検出手段と、前記許可フラッグが有効か、又は前記禁止フラッグが有効でないときに、可否フラッグを可にして出力し、前記許可フラッグが有効でなく、かつ前記禁止情報が有効であるときに、前記可否フラッグを不可にして出力する判定手段とを具備している。

【0027】

【発明の実施の形態】以下、本発明の実施の形態について、添付図面を参照して説明する。

【0028】(実施の形態1) 本実施の形態1におけるデータ制御方法について説明する。図1は本実施の形態1のデータ制御方法の概要を示す説明図である。本実施の形態1で言うデータ制御とは、コピー制御を意味する。図1(a)に示す様に、信号C1は画面全体に分散された信号であり、コピーの禁止情報31を示す。信号CEは画面の特定箇所挿入された信号であり、1回のコピーの許可情報32を示す。N回のコピーを許可する場合は、許可情報32をN個画面に挿入する。

【0029】信号C1は、例えば画面全体に分散され、視認することはできないものである。これに対して、信

10

20

30

40

50

号CEは、例えば画面の所定の角に挿入され、視認されなくても、視認されてもよい。

【0030】図1(b)はコピー不可の映像33を示す。図1(c)は1回コピー可の映像34を示し、画面右下に許可情報32が1つ挿入されている。図1(d)はコピー可の映像35を示し、画面全体に禁止情報31が画面に挿入されていない。

【0031】本実施の形態1が目的とするコピー制御とは、コピーフリーと、N回(以下の説明では $N=1$)コピー可と、コピー不可の3つの状態により映像信号の出力制御を行うものである。コピーフリー(コピー可)のときは、無条件でコピーを許可する。1回コピー可のときは、1回だけコピーを許可する。コピー不可のときは、映像の表示は許可してもコピーを一切禁止する。

【0032】コピー不可の映像33には、図1(b)のように禁止情報31を埋め込む。このコピー不可の映像33が記録装置に入力されたとき、許可情報32は検出されず、禁止情報31が検出される。この場合は映像33のコピーを禁止する。1回コピー可の映像34に対しては、図1(c)のように禁止情報31と許可情報32の両方を埋め込む。この映像34をコピーするときには、許可情報32が検出されるので、コピーを許可する。記録装置では、伝送路から該記録装置に転送されて来た映像34の許可情報32自身を削除して、映像34のコピーを開始する。ここで、許可情報32の削除においては、許可情報32を全て削除しても良いし、許可情報32の一部を削除しても良く、許可情報32として検出不可能な状態、つまり許可情報を無効にすることが目的である。例えば、許可情報32が8ビットの意味のある情報を持っていた場合、そのうちの1ビットを削除するだけでも良いし、8ビット全てを削除しても良い。あるいは、許可情報32が2つの情報の組み合わせにより構成されていた場合には、そのうちの片方を削除しても良い。

【0033】コピーした後の映像は許可情報32だけが取り除かれているので、禁止情報31が残り、コピー不可の映像33となる。

【0034】ただし、許可情報が2つ以上のN個埋め込まれていたN回コピー可の映像については、許可情報が1個削除されるので、 $(N-1)$ 回コピー可の映像になる。

【0035】コピーフリーの映像35には、禁止情報31も許可情報32も埋め込まない。このコピーフリーの映像35をコピーするときには、許可情報32も禁止情報31も検出されないので、無条件にコピーが許可される。

【0036】以上のようなコピー制御方法によれば、コピーの禁止と許可の制御だけでなく、N回だけコピーを許可するような制御を実現できる。さらに、コピーするときに禁止情報の埋込方法や禁止情報の削除方法を公開

する必要はない。このため、不正者が禁止情報を削除することが困難となる。また、コピー時に許可情報を埋め込まないので、その埋込方法は公開する必要はない。このため、不正者は許可情報を埋め込むことはできない。図1を用いた説明において、禁止情報を画面全体に埋め込むとしたが、これに限られるものではなく、画面の特定箇所に埋め込んでも良い。又図1を用いた説明において、許可情報を特定箇所に埋め込むとしたが、 $N=1$ に限定される場合には、これに限られず、画面全体に埋め込んでも良い。

【0037】次に、本実施の形態1のデータ制御方法を実現するための基本技術であるデータ制御情報埋込方法と、データ制御情報検出方法について、図2乃至図5を用いて説明する。

【0038】図2は本実施の形態1のデータ制御情報埋込方法を示すフローチャートである。図4は本実施の形態1のデータ制御情報検出方法を示すフローチャートである。

【0039】まず、図2で示すデータ制御情報埋込方法において、初期状態として、映像を(1)コピー不可、(2)1回コピー可、(3)コピーフリーの内、いずれの状態かを示す変数`Status`を設定する。まずステップS1では、`Status`がコピーフリーかどうかを判定し、コピーフリーの場合には処理を終了し、コピーフリーでない場合には、ステップS2に分岐する。ステップS2では、禁止情報31を映像中に埋め込む。

【0040】この埋め込み処理は、例えば従来技術のコピー制御情報の埋込方法など、映像中に1ビット以上の情報を埋め込むための任意の埋込方法で良い。特に、埋込方法がその検出方法よりも複雑である方法であればなお良く、その制限の元であれば、埋め込み方法によって本発明の効果が損なわれることはない。このような映像に情報を埋め込む方法は、電子透かし(Water Mark)と呼ばれ、従来技術で示した方法以外にも数多くの方法が知られている。例えば、日経エレクトロニクスの1997年2月24日号(電子透かしがマルチメディア時代を守る)に紹介されている方法などがある。次のステップS3に進むと、`Status`が1回コピー可か否かを判定し、1回コピー可でない場合に処理を終了し、1回コピー可の場合にはステップS4に分岐する。

【0041】ステップS4では、許可情報32を映像中に埋め込む。このステップS4は、例えば図3のフローチャートに示す様な処理であり、このフローチャートを参照して、このステップS4の許可情報の埋め込み処理を詳細に説明する。

【0042】まず、ステップS21では、情報を埋め込む映像の画素からその映像と一意に対応するコードMを抜き出す。コードMの抜き出し処理は、例えば映像中からk個の所定の各画素を選び、これらの画素のデータの

MSB（最上位ビット）をkビットのコードMとする方法で実現できる。しかしこれに限定されず、映像から8×8画素のブロックをk個選び、これらのブロックの輝度値をkビットのコードMとする方法、映像の周波数成分を計算してその低周波成分を用いる方法など、映像からデジタルデータを一意に抜き出せる方法であれば、任意の方法で良い。

【0043】次のステップS22では、コードMを用いてデジタル署名f(M)を作成する。ここでデジタル署名について詳細に説明しておく。ユーザAが映像の送信者、ユーザBが映像の受信者とし、ユーザAからユーザBに映像のコードMを署名C=f(M)に変換して送信する場合を考える。このとき、ユーザAは署名Cを作成して映像を送信し、ユーザBはその署名を認証、即ちその署名が正しいか否かを検証する。

【0044】本実施の形態1に要求されるデジタル署名とは、次の性能が満たされればなんでも良い。

【0045】(1) ユーザBは署名Cを容易に認証できること。

【0046】(2) ユーザAは署名Cの作成は容易だが、ユーザA以外の者は署名Cの作成は困難であること。

【0047】このデジタル署名の具体的な方法として、公開鍵暗号を利用する方法がある。ユーザAは、署名を行う関数として署名関数D（第1の暗号鍵）を用意し、認証を行う関数として認証関数E（第2の暗号鍵）を用意する。ここで認証関数Eは署名関数Dの逆関数になるよう設定する。ユーザAは署名関数Dを用いて、コードMから署名Cを、 $C=D(M)$ により作成する。ユーザBは認証関数Eを用いて、 $E(C)$ がMと一致するか否かを検証する。即ち認証関数Eは署名関数Dの逆関数なので、Cが正しい署名であれば、 $E(C)=E(D(M))=M$ となり、Cが正しい署名でなければ、 $E(C)$ とMとは一致しない。

【0048】ここで公開鍵暗号では、公開された認証関数Eから、秘密である署名関数Dを求めるのが困難であるという仕組みを、数学的な手法を用いて実現している。この実現例としては、RSA暗号、ElGamal暗号等を利用したものがある。RSA暗号では、署名関数Dを次の(1)式で定義する。

$$D(M)=M^d \bmod n \quad \cdots (1)$$

【0049】また認証関数Eは次の(2)式で定義する。

$$E(C)=C^e \bmod n \quad \cdots (2)$$

【0050】ここでmod nは、nによる剰余演算、即ちnで割った余りの整数を意味する(1)、(2)式におけるn、e、dは、EがDの逆関数になるよう選択される。即ち次の(3)式が成立するよう選択される。

$$E(C)=C^e \bmod n=(M^d)^e \bmod n \\ =M^{de} \bmod n=M \quad \cdots (3)$$

ユーザAは、大きな素数p、qを用意し、 $n=p \times q$ とする。次に $(p-1) \times (q-1)=\phi(n)$ なるオイラーの関数 $\phi(n)$ を定義する。次に関数 $\phi(n)$ と互いに素となる整数eを適当に設定する。即ち、 $\phi(n)$ とeは、その最大公約数が1になる。そして次の(4)式が成立するようにdを決定する。

$$e \times d \bmod \phi(n)=1 \quad \cdots (4)$$

このように決定されたe、dを用いれば、前述した(3)式が成立する。

【0051】ユーザAはnとeとを公開し、d、p、qを秘密にする。従って認証関数Eは公開されるが、署名関数Dは秘密にされる。pとqを知っているユーザAは、(4)式を用いてeからdを求めることができる。しかしpとqを知らないユーザBは、nとeからdを求めることが困難となる。

【0052】理解を容易にするため、ごく簡単な数値例を示す。例えば素数としてp=5、q=11を選ぶと、 $n=55$ 、 $\phi(n)=40$ となる。次にe=7を選ぶと、(4)式から、 $7 \times 23 \bmod 40=1$ となり、 $d=23$ が得られる。ユーザAは、 $n=55$ とe=7を公開し、p=5、q=11、d=23を秘密にする。

【0053】例えばM=42に対する署名は、次の(5)式のように計算される。

$$D(M)=42^{23} \bmod 55=3 \quad \cdots (5)$$

【0054】これよりC=3となる。ユーザBは公開されている認証関数を用いて、次の(6)式の計算を行う。

$$E(C)=3^7 \bmod 55=42 \quad \cdots (6)$$

【0055】この結果、E(C)は当初のM=42と一致するので、正しい署名であることが認証される。

【0056】ここでは、簡単のために、nを構成する素数p、qとして小さい値を選んだが、暗号の安全性を高めるために、実際のnは512ビット程度の大きさが用いられる。p、qの値が256ビット幅としても、その大きさは10進数に換算して、77～78桁程度の巨大な値になる。

【0057】以上の説明は、公開鍵暗号を用いたデジタル署名であるが、これ以外にも、ナップザック問題に基づくデジタル署名や、ゼロ知識会話型証明を適用したデジタル署名などがあり、参考文献である辻井、笠原著「暗号と情報セキュリティ」（昭昇堂発行）に記載されている。

【0058】さて、図2及び図3のフローチャートについて引き続き説明する。図3のステップS22で、コードMを用いてデジタル署名f(M)を作成した後、ステップS23で映像中に署名f(M)を埋め込む。映像中への署名f(M)の埋め込みの方法として、0は白、1は黒というような可視的なパターンで映像の端に埋め込む方法がある。しかしこの方法に限定せず、映像中から選択した画素のLSB（最下位ビット）を署名f(M)

で置き換える方法、映像のブランキング区間に埋め込む方法、容易に削除可能な電子透かしを用いる方法など、複数ビットのコードを埋め込める方法であれば、任意の方法で良い。

【0059】この様な許可情報の埋め込みの処理は、映像から一意に導き出せるコードMを元にしたデジタル署名を許可情報として用いているので、秘密鍵dがなければ第3者が同じ署名を作成することは困難であり、新たに許可情報の埋め込みはできない。

【0060】本実施の形態1のコピー制御情報埋込方法により、コピーフリーの場合には、映像には何も埋め込まず、1回コピー可の場合には禁止情報と1つの許可情報を映像に埋め込む。そしてコピー不可の場合には禁止情報のみを映像に埋め込む。

【0061】次に、図4を参照して、像からコピー制御情報を検出するための本実施の形態1のデータ制御情報検出方法について説明する。

【0062】まず、ステップS5では、映像から許可情報32の検出を行う。このステップS5は、例えば図5のフローチャートに示す様な処理であり、このフローチャートを参照して、このステップS5の許可情報の検出処理を詳細に説明する。

【0063】図5のステップS24において、映像に埋め込まれた署名f(M)を検出する。次のステップS25では、映像からコードMを抜き出す。このコードMの抜き出しは、図3のステップS21でコードMを抜き出したのと同じ処理でできる。

【0064】次のステップS26では、デジタル署名の認証を行う。このデジタル署名の認証は、ステップS22で作成した署名の認証である。例えば、RSA暗号の認証の場合、公開情報nと公開鍵eを用いる。署名f(M)をCとすると、署名の認証のための関数は前述した(2)式で表される。この結果が、(3)式で示すようにMとなれば、認証可であり、Mと一致しなければ認証不可である。

【0065】認証可であれば、許可情報が埋め込まれているので、ステップS27に進み、許可フラグに1を代入する。ステップS26で認証不可であれば、許可情報が埋め込まれていないので、ステップS28に進み、許可フラグに0を代入する。本実施の形態1では上記のように許可フラグを生成したが、許可情報が埋め込まれている状態と、埋め込まれていない状態とを識別できる信号であれば、何でも良い。

【0066】この様に図4のステップS5で許可情報を検出した後、ステップS6に進み、許可フラグを判定する。許可フラグが1の場合にはステップS7に分岐し、0の場合にはステップS8に分岐する。ステップS7では許可情報の削除を行う。この許可情報の削除は、ステップS4で埋め込まれた許可情報を、映像から取り除く処理であり、先程示したように、許可情報の少なくとも

一部を削除する。ステップS7の処理後、ステップS11に進み、コピー可否フラグを1にする。

【0067】ステップS8では、禁止情報を検出する。これはステップS2で埋め込まれた禁止情報を検出することである。ここでは禁止情報がある場合には禁止フラグを1にし、ない場合には禁止フラグを0にする。その後ステップS9に進み、禁止フラグの判定を行う。禁止フラグが1の場合にはステップS10へ分岐し、禁止フラグが0の場合にはステップS11へ分岐する。禁止フラグの生成方法は、上記の方法に限らず、禁止情報が埋め込まれている状態と、埋め込まれていない状態を識別できる信号であれば、何でも良い。

【0068】ステップS10ではコピー可否フラグを0にし、ステップS11ではコピー可否フラグを1に設定する。ここで、コピー可否フラグは、0がコピー禁止、1がコピー許可を示す信号である。なお、コピー可否フラグは、コピーの禁止と許可を識別できる信号であれば、任意の形態で良い。

【0069】本実施の形態1のデータ制御情報検出方法により、許可情報が埋め込まれた映像は、許可情報が削除された後でコピーが許可される。許可情報も禁止情報も埋め込まれていない映像は、コピーが許可される。許可情報が埋め込まれておらず、禁止情報が埋め込まれている映像は、コピーが禁止される。

【0070】以上説明したように、本実施の形態1では、1回コピー可からコピー不可への変化を、許可情報の埋め込みと削除で実現している。さらにこの許可情報の埋め込みはデジタル署名に基づいており、削除や検出は容易であるが、秘密鍵dを知らない者にとっては、許可情報の埋め込みは困難である。このため不正にコピー許可に変更(書換え)することは困難である。さらに、禁止情報は許可情報と別の方法で埋め込んでおり、ユーザBにはその検出方法のみを公開又は提供すれば良いので、ユーザAは、その埋め込みや削除の方法を秘密にできる。

【0071】また、本実施の形態1によれば、コピーの禁止と許可だけでなく、一回だけコピーを許可するような制御を実現できる。このため、従来と比べて不正が困難なデータ制御方法、あるいはデータ制御情報埋込方法及びデータ制御情報検出方法を実現できる。

【0072】また、本実施の形態1では、1回コピー可を実現する方法について述べたが、コピー制御情報を埋め込む時に許可情報をN(Nは2以上の整数)回埋め込み、検出するときには許可情報が何個検出されても1個だけ削除することにより、N回コピー可という制御も実現可能である。

【0073】なお、以上の説明では、コピーの禁止、1回許可、N回許可というデータ制御方法について説明したが、これに限られるものではなく、映像の再生の禁止、1回許可、N回許可という制御、更には映像の編集

又は加工といったデータ処理や、映像の表示も同様に制御することができる。

【0074】また、映像信号を処理の対象としているが、音声信号や文書を処理の対象としてもよく、同様の効果が得られる。

【0075】更に、許可信号として映像から一意に得られるコードMを元にしたデジタル署名を用いているが、これに限られるわけではなく、任意の埋め込み方法を用いることができる。即ち、ユーザBに埋め込み方法を公開せず、削除と検出の方法のみを公開すれば良い。削除や検出の方法から、埋め込みの方法が類推できない方法や、削除や検出と比べて埋め込み処理の計算量が多いか、又は回路規模が複雑であるような方法であれば、更に不正に対して強くすることができる。この時、映像から一意に得られるコードMを元にして許可情報を作成することにより、映像と許可情報を1対1に対応させることができ、許可情報の不正な作成を困難にする。

【0076】許可情報の埋め込み方法の他の例としては、許可情報が第1の許可情報と第2の許可情報の2つから構成され、第1の許可情報を第1の埋め込み方法を用いて映像中に埋め込むと同時に、第2の許可情報を第2の埋め込み方法を用いて映像に埋め込む方法がある。ここで、第1の埋め込み方法は削除が難しい方法、すなわち禁止情報の埋め込み方法に用いたのと同様の方法で埋め込みを行い、第2の埋め込み方法は画面の端に可視的に埋め込むなどの削除が容易な方法で埋め込みを行う。映像のコピーに際しては、第1の許可情報と第2の許可情報の両方がそろって検出されたときに始めてコピー可とし、第2の許可情報のみを削除する。このように第1の許可情報と第2の許可情報の組み合わせにより、検出と削除が容易であるが、その埋め込みが困難であるような埋め込み方法を実現することが可能となる。ここで示した第1の埋め込み方法は、禁止情報の埋め込み方法と全く同じ方法でも良いし、異なる方法でも良い。

【0077】第1と第2の2つの許可情報を構成する方法としては、コードMを変換係数により変換処理した結果と、変換係数のいずれか一方を第1の許可情報とし、もう一方を第2の許可情報とする方法がある。ここで、変換処理とは、変換係数との加減乗除などの算術計算や、変換係数との論理演算や、変換係数を鍵とした暗号化処理や、変換係数を遅延量とした遅延処理など、変換係数の値によってその処理結果が変わるような処理であれば任意の方法を取ることが可能である。特に、コードMと変換結果から変換係数を求めることが困難であるような変換処理が望ましく、不正に対して強いという効果がある。これは、変換処理の方法を秘密にすることにより実現できる。

【0078】（実施の形態2）本発明の実施の形態2として、実施の形態1で説明したデータ制御方法を実現するためのデータ制御システム、及び該システムにおける

データ制御情報埋込装置とデータ制御情報情報検出装置を示す。

【0079】図6は、本実施の形態2におけるデータ制御システムの構成図である。このデータ制御システムは、データ制御情報埋込装置41、データ制御情報検出装置42、伝送部43、記録部44、記録媒体45を含んで構成される。

【0080】データ制御情報埋込装置41では、映像信号を入力してコピー制御情報を埋め込み、この情報が埋め込まれた映像信号を伝送部43に出力する。

【0081】伝送部43による伝送方法として、衛星や地上波などを利用した無線によるデジタル伝送又はアナログ伝送が有る。又、電話線や同軸ケーブル、ツイストペアケーブル、光ケーブルなどを利用した有線によるデジタル伝送又はアナログ伝送がある。更には、磁気ディスク、光ディスク、CD、DVD、DVC、VCRなどのデジタル又はアナログの記録メディアも、該記録メディアから映像信号がビットストリームとして再生されるので伝送部43と考える。

【0082】伝送部43を介して伝送もしくは再生された映像信号は、データ制御情報検出装置42に輸入される。データ制御情報検出装置42では、コピー制御情報を検出し、コピー許可かコピー禁止かを示す記録可否フラグと映像情報を出力し、これらの情報が記録部44に輸入される。

【0083】記録部44は、記録可否フラグがコピー許可を示す場合は、記録媒体45に映像情報の記録を許可し、コピー禁止を示す場合には記録を行わない。ここで記録媒体45は、磁気ディスク、光ディスク、CD、DVD、DVC、VCRなどのデジタル又はアナログの記録メディアなど、データの記録を行う媒体であれば任意の媒体で良い。

【0084】データ制御情報埋込装置41は、禁止情報埋込手段411と許可情報埋込手段412を有している。

【0085】データ制御情報埋込装置41において、禁止情報埋込手段411は、一回コピー可又はコピー禁止の情報を埋め込みたい場合に、入力した映像信号に禁止情報を埋め込む。この埋め込み処理は、図2のステップS2の処理と同じである。次に、許可情報埋込手段412は、1回コピー可の場合に、許可情報を映像信号中に埋め込む。この許可情報埋込手段412の動作については後述する。この様なデータ制御情報埋込装置41の動作により、コピーフリーの場合は映像に何も埋め込まれず、一回コピー可の場合には映像に禁止情報と許可情報とが埋め込まれ、コピー不可の場合には映像に禁止情報が埋め込まれる。

【0086】データ制御情報検出装置42は、禁止情報検出手段421、許可情報検出・削除手段422、判定手段423を有している。

【0087】データ制御情報検出装置 4 2 において、許可情報検出・削除手段 4 2 2 は映像信号から許可情報の検出及び削除を行う。許可情報が検出された場合には 1 を、検出されない場合には 0 を示す許可フラグが出力される。許可情報検出・削除手段 4 2 2 の動作については後述する。

【0088】禁止情報検出手段 4 2 1 は、許可情報検出・削除手段 4 2 2 から映像信号を入力すると、埋め込まれた禁止情報の有無を調べる。ここで禁止情報が検出された場合には 1 を、検出されない場合には 0 を示す禁止フラグが出力される。許可フラグと禁止フラグの値は判定手段 4 2 3 に入力される。判定手段 4 2 3 は許可フラグが 1 の場合、又は禁止フラグが 0 の場合には、コピー許可を示す記録可否フラグを出力する。また許可フラグが 0 でかつ禁止フラグが 1 の場合には、コピー禁止を示す記録可否フラグを出力する。

【0089】以上のデータ制御情報検出装置 4 2 の動作により、許可情報が埋め込まれた映像は許可情報が削除された後でコピーが許可される。また、許可情報も禁止情報も埋め込まれていない映像は、コピーが許可される。更に許可情報が埋め込まれておらず、禁止情報が埋め込まれている映像は、コピーが禁止される。

【0090】次に、許可情報埋込手段 4 1 2 及び許可情報検出・削除手段 4 2 2 の構成と動作について図 7 及び図 8 を用いて説明する。

【0091】図 7 に示すように許可情報埋込手段 4 1 2 は、署名埋込手段 5 1、コード抽出手段 5 2、署名手段 5 3 を含んで構成される。

【0092】許可情報埋込手段 4 1 2 においては、まずコード抽出手段 5 2 が、映像信号から一意に導き出せるコード M を生成して署名手段 5 3 に出力する。署名手段 5 3 はコード M をデジタル署名 $f(M)$ に変換し、署名埋込手段 5 1 に出力する。次に署名埋込手段 5 1 は、映像信号中にデジタル署名 $f(M)$ を埋め込む。許可情報を埋め込まない場合には、デジタル署名 $f(M)$ の埋め込み処理は行わない。ここで、コード抽出手段 5 2 におけるコード M の生成方法、署名手段 5 3 における署名 $f(M)$ の生成方法、署名埋込手段 5 1 における署名の埋め込み方法は、図 3 のステップ S 2 1、S 2 2、S 2 3 の処理と夫々同様である。

【0093】図 8 に示すように許可情報検出・削除手段 4 2 2 は、署名拔出・削除手段 5 4、コード抽出手段 5 5、認証手段 5 6 を含んで構成される。

【0094】許可情報検出・削除手段 4 2 2 においては、署名拔出・削除手段 5 4 がデジタル署名 $f(M)$ を映像信号から抜き出し、映像信号からデジタル署名 $f(M)$ の少なくとも一部を削除する。次に、コード抽出手段 5 5 は、コード抽出手段 5 2 と同様に映像信号からコード M を生成して認証手段 5 6 に出力する。次に、認証手段 5 6 は、コード M を基にデジタル署名 $f(M)$ を

認証し、記録許可を示す記録可否フラグを出力する。また認証されなければ、記録禁止を示す記録可否フラグを出力する。ここで、署名拔出・削除手段 5 4 における署名の抜き出し方法、コード抽出手段に 5 5 におけるコード M の生成方法、認証手段 5 6 における認証方法は図 5 で説明したものと夫々同様である。

【0095】以上のように本実施の形態 2 によれば、コピーの禁止と許可だけでなく、1 回だけコピーを許可するような制御を実現でき、従来の方法に比べて、不正がより困難であるデータ制御システム、及び該システムにおけるデータ制御情報埋込装置とデータ制御情報検出装置を実現できる。

【0096】なお、本実施の形態 2 では、1 回コピー可を実現する方法について述べたが、コピー制御情報を埋め込む時に許可情報を N (N は 1 以上の自然数) 回埋め込み、検出するときには許可情報が何個検出されても、1 個だけ削除することにより、N 回コピー可を実現することができる。

【0097】また、コピー禁止情報の埋め込みと検出の方法について述べたが、再生禁止情報の埋め込みと検出の方法も同様に実現でき、再生の制御も行える。さらに、コピーの制御と再生の制御も同時に実現可能である。

【0098】コピー制御情報埋込み装置 4 1 については図 6 に示すような構成としたが、これに限られるものではない。禁止情報埋込手段 4 1 1 と許可情報埋込手段 4 1 2 の順序が逆でも良く、コピー不可の映像には少なくとも禁止情報を埋め込み、1 回コピー可の映像には禁止情報と許可情報の両方を埋め込むような任意の構成の装置により実現可能である。

【0099】コピー制御情報検出装置 4 2 のについては、図 6 に示すような構成としたが、これに限られるものではない。許可情報検出削除手段 4 2 2 の前段の映像信号が禁止情報検出手段 4 2 1 に入力されるような構成でも良いし、許可情報検出削除手段 4 2 2 が許可情報検出手段と許可情報削除手段に分離されているような構成でも良く、許可情報が検出されるとコピーを許可して許可情報を削除し、禁止情報が検出されるとコピーを禁止するような任意の構成の装置により実現可能である。

【0100】以上の説明では、許可信号として映像から一意に得られるコード M を元にしたデジタル署名を用いているが、これに限られるわけではなく、任意の埋め込み方法を用いることができる。即ち、ユーザ B に埋め込み方法を公開せず、削除と検出の方法のみを公開すれば良い。削除や検出の方法から、埋め込みの方法が類推できない方法や、削除や検出と比べて埋め込み処理の計算量が多いか、又は回路規模が複雑であるような方法であれば、更に不正に対して強くすることができる。この時、映像から一意に得られるコード M を元にして許可情報を作成することにより、映像と許可情報を 1 対 1 に対

応させることができ、許可情報の不正な作成を困難にする。

【0101】許可情報の埋め込み方法の他の例としては、許可情報が第1の許可情報と第2の許可情報の2つから構成され、第1の許可情報を第1の埋め込み方法を用いて映像中に埋め込むと同時に、第2の許可情報を第2の埋め込み方法を用いて映像に埋め込む方法がある。ここで、第1の埋め込み方法は削除が難しい方法、すなわち禁止情報の埋め込み方法に用いたのと同様の方法で埋め込みを行い、第2の埋め込み方法は画面の端に可視的に埋め込むなどの削除が容易な方法で埋め込みを行う。映像のコピーに際しては、第1の許可情報と第2の許可情報の両方がそろって検出されたときに始めてコピー可とし、第2の許可情報のみを削除する。このように第1の許可情報と第2の許可情報の組み合わせにより、検出と削除が容易であるが、その埋め込みが困難であるような埋め込み方法を実現することが可能である。ここで示した第1の埋め込み方法は、禁止情報の埋め込み方法と全く同じ方法でも良いし、異なる方法でも良い。

【0102】第1と第2の2つの許可情報を構成する方法としては、コードMを変換係数により変換処理した結果と、変換係数のいずれか一方を第1の許可情報とし、もう一方を第2の許可情報とする方法がある。ここで、変換処理とは、変換係数との加減乗除などの算術計算や、変換係数との論理演算や、変換係数を鍵とした暗号化処理や、変換係数を遅延量とした遅延処理など、変換係数の値によってその処理結果が変わるような処理であれば任意の方法を取ることが可能である。特に、コードMと変換結果から変換係数を導くことが困難であるような変換処理が望ましく、不正に強いという効果が得られる。これは、変換処理の方法を秘密にすることにより実現できる。

【0103】なお、上記各実施形態1及び2においては、データ制御情報埋め込み方法あるいはデータ制御情報埋め込み装置は、ステータスがコピーフリーの時に禁止情報も許可情報も埋め込まないとしたが、これに限られるものではない。ステータスがコピーフリーを示すときには、コピーフリーを示す情報を埋め込んで良く、同様の効果が得られる。

【0104】また、データ制御情報検出方法あるいはデータ制御情報検出装置においては、コピー制御情報が検出されないときには、コピーを許可するとしたが、これに限られるものではない。何も情報が検出されないときには、コピー禁止としても良い。また、コピーフリーを示す情報が検出されたときにはコピー可とするような構成としても良く、同様の効果が得られる。

【0105】

【発明の効果】以上の様に、本発明によれば、コピーフリーとコピー禁止だけでなく、データに許可情報が検出されたとき、N回のコピーのみを許すことができる。そ

して不正行為が困難なデータ制御方法を実現できる。

【0106】1実施形態によれば、データの作り手側で、許可情報をデジタル署名を用いて挿入しているため、データを入手した側での許可情報の改ざんは不可能となる。

【0107】1実施形態によれば、コピーフリーとコピー禁止の制御だけではなく、N回のコピーを許可する情報も埋め込むことができる。

【0108】また、1実施形態によれば、データから一意に得られるコードを元に許可情報を生成しているため、許可情報はデータと1対1に対応し、許可情報の改ざんを困難にすることが出来る。

【0109】1実施形態によれば、許可情報がデジタル署名を用いて挿入されているため、データを入手した側での許可情報の改造は不可能となる。

【0110】1実施形態によれば、許可情報の挿入されたデータが入力されたとき、コピー回数をN回に制限し、禁止情報のみが挿入されたデータが入力されたとき、コピーを禁止することができる。

【0111】1実施形態によれば、データから一意に得られるコードを元にした許可情報が検出されたときのみ、コピーを許可する。

【0112】1実施形態によれば、デジタル署名が認証されたときにのみ、コピーが許可される。

【0113】1実施形態によれば、データより許可情報が検出されたとき、そのデータを記録媒体に記録することができる。

【0114】1実施形態によれば、データに禁止情報のみが検出されたとき、データ処理を禁止し、許可情報が検出されたとき、N回のデータ処理を許すことができる。

【0115】1実施形態によれば、データ処理の禁止の制御だけではなく、N回のデータ処理を許可する情報も埋め込むことができる。

【0116】1実施形態によれば、許可情報の挿入されたデータが入力されたとき、データ処理回数をN回に制限し、禁止情報のみが挿入されたデータが入力されたとき、データ処理を禁止することができる。

【0117】1実施形態によれば、許可情報の挿入されたデータが入力されたとき、データ処理回数をN回に制限し、禁止情報のみが挿入されたデータが入力されたとき、データ処理を禁止することができる。

【図面の簡単な説明】

【図1】実施の形態1のデータ制御方法の概要を示す説明図である。

【図2】実施の形態1のデータ制御情報埋込方法を示すフローチャートである。

【図3】図2のデータ制御情報埋込方法の1処理を示すフローチャートである。

【図4】実施の形態1のデータ制御情報検出方法を示す

21

フローチャートである。

【図 5】図 4 のデータ制御情報検出方法の 1 処理を示すフローチャートである。

【図 6】本実施の形態 2 におけるデータ制御システムの構成図である。

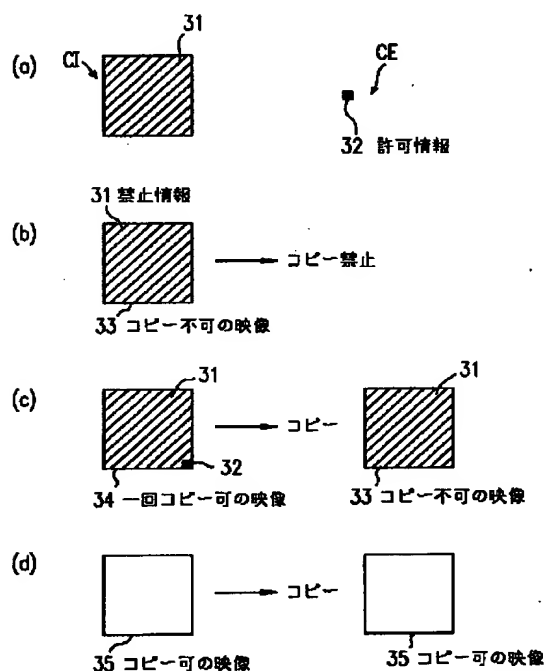
【図 7】図 6 のデータ制御システムにおける許可情報埋込手段の構成図である。

【図 8】図 6 のデータ制御システムにおける許可情報検出手段の構成図である。

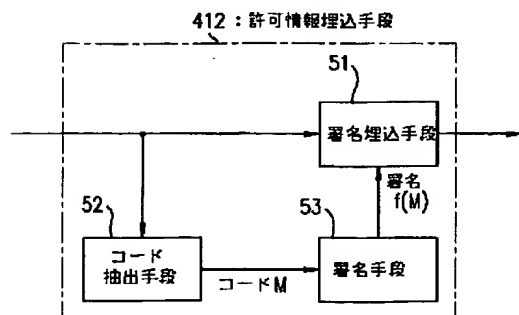
【符号の説明】

- 4 1 データ制御情報埋込装置
4 2 データ制御情報検出装置
4 3 伝送部

【図 1】



【図 7】

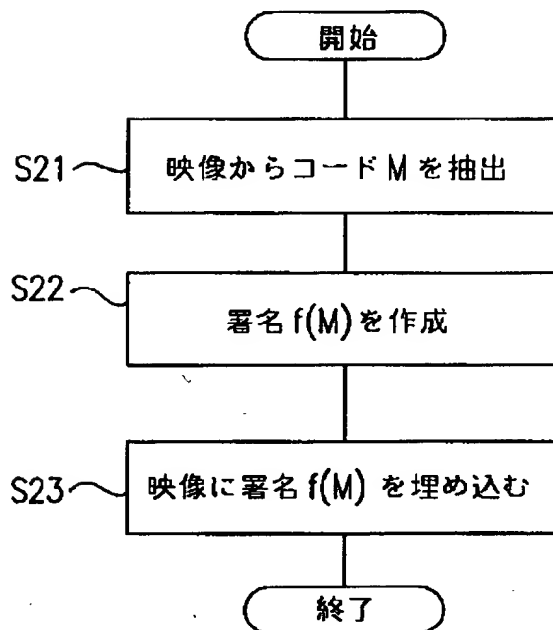


22

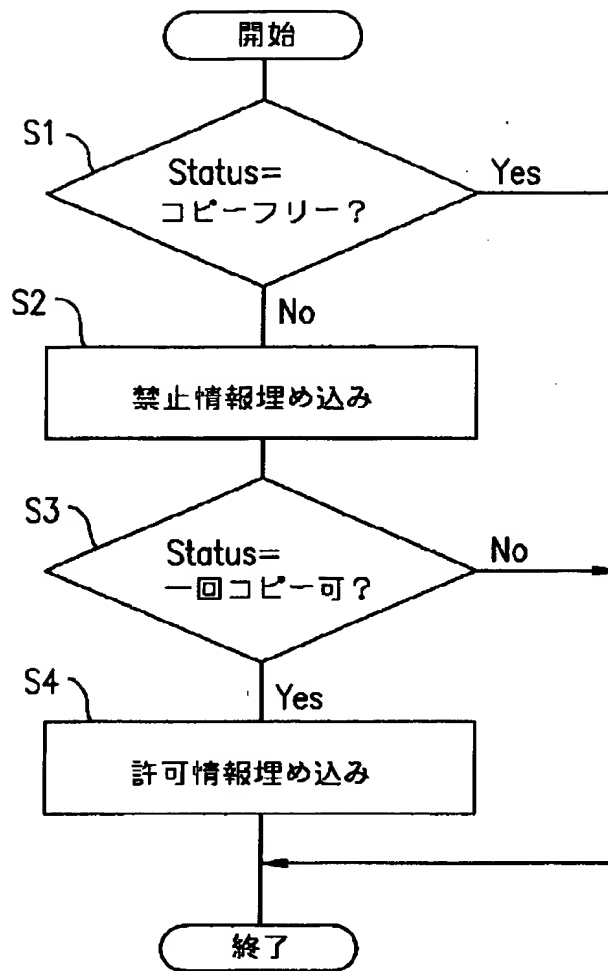
- * 4 4 記録部
4 5 記録媒体
5 1 署名埋込手段
5 2, 5 5 コード抽出手段
5 3 署名手段
5 4 署名抽出・削除手段
5 6 認証手段
4 1 1 禁止情報埋込手段
4 1 2 許可情報埋込手段
10 4 2 1 禁止情報検出手段
4 2 2 許可情報検出・削除手段
4 2 3 判定手段

*

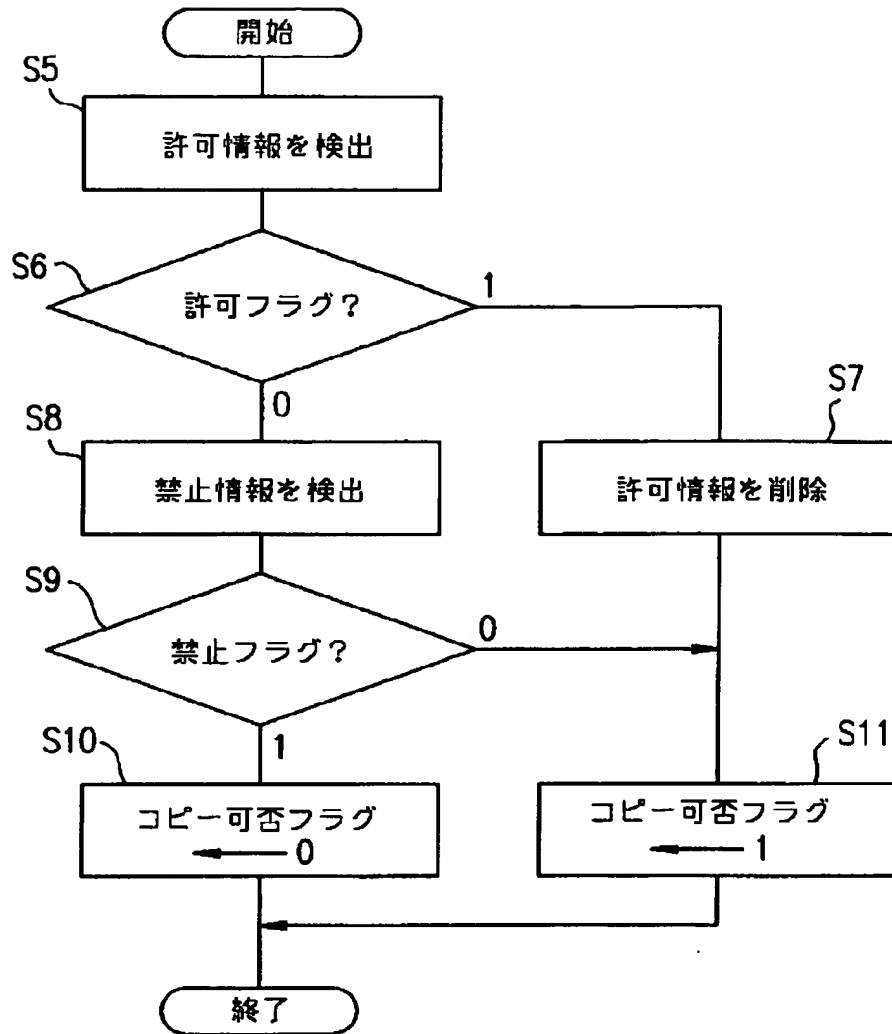
【図 3】



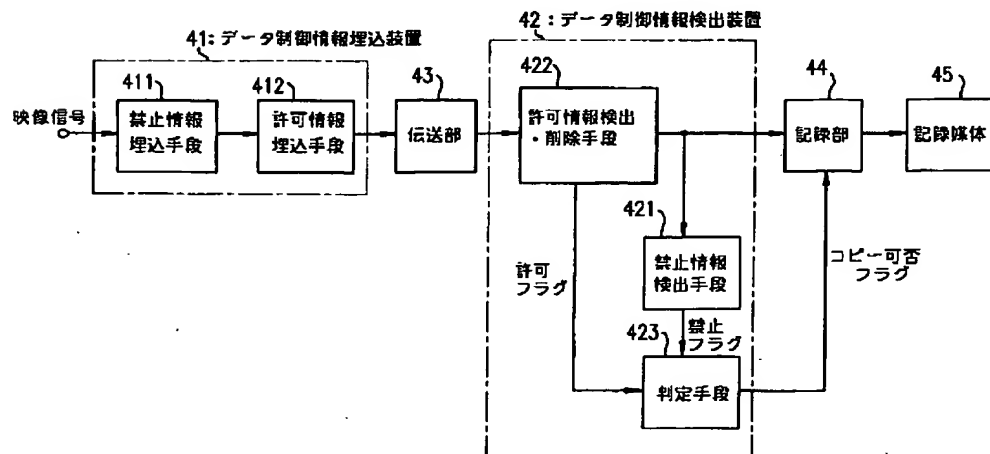
【図 2】



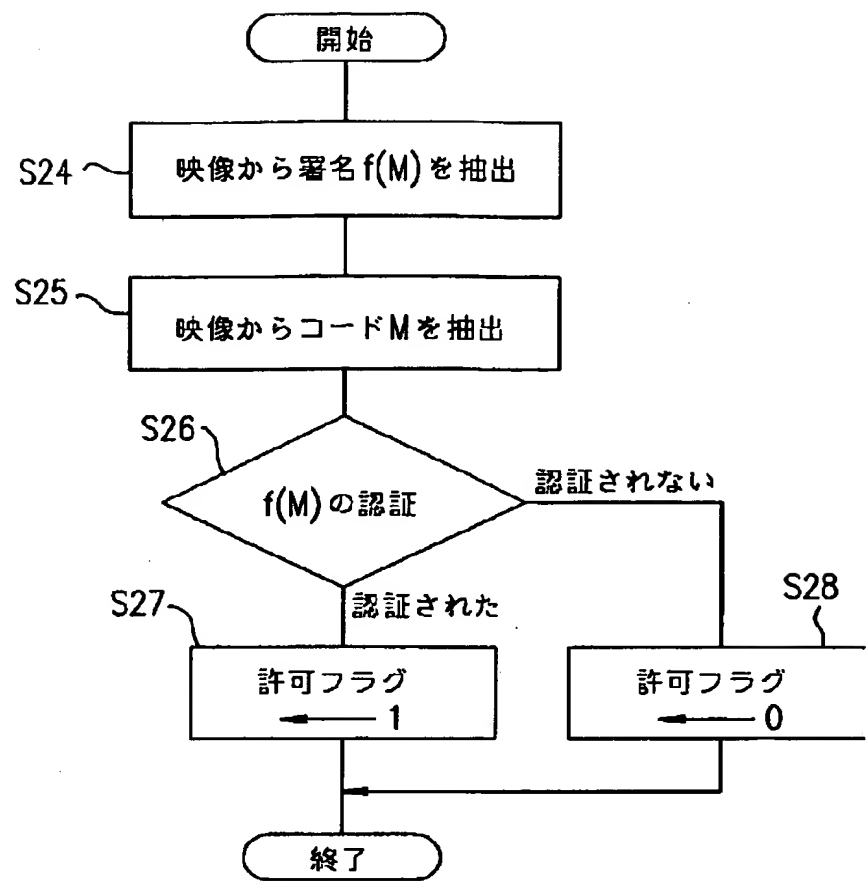
【図 4】



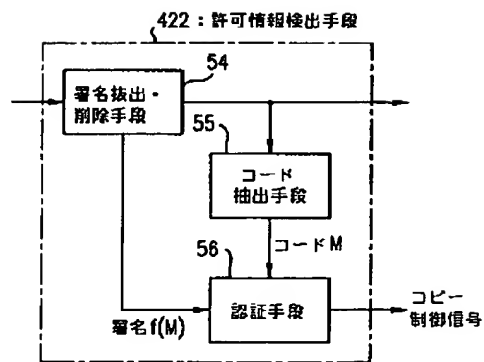
【図 6】



【図 5】



【図 8】



フロントページの続き

7/08
7/081

7/08

Z